Project no.:	**ICT-FP7-STREP-214755**
Project full title:	**Quantitative System Properties in Model-Driven Design**
Project Acronym:	**QUASIMODO**

Deliverable no.: D1.1

Title of Deliverable: Modelling Quantitative System Aspects

Contractual Date of Delivery to the CEC:	**Month 12**
Actual Date of Delivery to the CEC:	**Month 12 (February 1, 2009)**
Organisation name of lead contractor for this deliverable:	**P02 ESI**
Author(s):	**Holger Hermanns, David Jansen, Rom Langerak, Julien Schmaltz, and Frits Vaandrager**
Participant(s):	**P02 ESI, P04 RWTH, P05 Saarland University**
Work package contributing to the deliverable:	**WP 1**
Nature:	**R**
Version:	**1.0**
Total number of pages:	**12**
Start date of project:	1 Jan. 2008 **Duration:** 36 month

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)

Dissemination Level

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Abstract:

This deliverable describes the results of the QUASIMODO project on modelling quantitative system aspects.

Keyword list: AADL, Arcade, architectural dependability evaluation, cost-bounded reachability, priced priced/weighted timed automata, probabilistic timed automata, probabilistic timed automata, probabilistic hybrid systems.

Contents

Abbreviations

AAU: Aalborg University, DK

CNRS: National Center for Scientific Research, FR

ESI: Embedded Systems Institute, NL

ESI/RU: Radboud University Nijmegen, NL

ESI/UT: University of Twente, NL

RWTH: RWTH Aachen University, D

SU: Saarland University, D

1 Introduction

This deliverable presents an overview of the work on modelling of quantitative systems aspects that has been carried out within Task 1.2 during the first year of the QUASIMODO project. In full agreement with the *Description of Work*, we have worked on four different topics:

1. Stochastic component-based modelling
2. Probabilistic timed modelling
3. Stochastic hybrid modelling
4. Resources modelling

The next sections summarize the results that we obtained in these respective areas, and discuss their relevance for the project.

2 Stochastic component-based modelling

2.1 Rich interfaces for dependability

Participants

- Hichem Boudali, ESI/UT
- Pepijn Crouzen, SU
- Boudewijn Haverkort, ESI/UT
- Matthias Kuntz, ESI/UT
- Mariëlle Stoelinga, ESI/UT

Results We have proposed a formally well-rooted and extensible framework for dependability evaluation: Arcade (architectural dependability evaluation). It has been designed to combine the strengths of previous approaches to the evaluation of dependability. A key feature is its formal semantics in terms of Input/Output-Interactive Markov Chains, which enables both compositional modeling and compositional state space generation and reduction. The latter enables great computational reductions for many models. The Arcade approach is extensible, hence adaptable to new circumstances or application areas. This new modeling approach has been provided with a formal semantics and has been illustrated on several case studies. See [2, 3, 4].

Perspective Our results on Arcade have also been included in Deliverable D1.2. This work links existing ideas from concurrency theory and probabilistic systems to the area of dependability evaluation, opening up a new rich class of potential applications.

2.2 System and software co-engineering: performance and verification

Our results [8] on the design notation AADL have also been included in Deliverable D1.2. We refer to Deliverable D1.2 for a description of this work. However, as quantitative aspects play a very important role in this work (the so-called error model essentially consists of probabilistic automata) we think it is relevant to also mention it here.

Perspective In this work we link AADL, the architecture analysis and design language of the Society of Automotive Engineers, to the world of probabilistic automata and model checking. Thus we make formal analysis techniques available to an important application area.

3 Probabilistic timed modelling

3.1 A translational approach to checking probabilistic timed automata

Participants

- Arnd Hartmans, SU
- Holger Hermanns, SU

Results The formalism of probablistic timed automata (PTA) combines discrete probabilities and nondeterministic time. We are working towards model-checking of PTA using the language MODEST [1]. This language includes features such as exception handling, dynamic parallelism and recursion. A large (and compositionally closed) subset of MODEST maps to PTA.

In contrast to purely symbolic techniques [11] relying on regions or zones to represent continuous time, we use an integral semantics [10] which relies on (bounded) integer variables to represent clocks. Still, probabilistic and expected reachability properties are preserved for PTA with closed, diagonal-free clock constraints. This allows checking a considerable set of interesting properties by first applying the integer semantics, resulting in a purely probabilistic model, and then using existing and proven probabilistic model checkers.

We have developed a tool that automatically translates MODEST models – if corresponding to PTA – to input models for the PRISM probabilistic model checker (and other tools) using the integral representation of time. The translation does not flatten parallelism and support almost all features of MODEST, including exception handling and (tail-)recursive process calls. Properties may be specified for the MODEST model, and include the generation of rewards structures (for expected reachability) and observer modules (for action-based properties). We are working on methods to overcome limitations imposed by PRISM's static module structure to allow (some form of) dynamic parallelism as well. As a testbench, the tool has been applied to the BRP (bounded retransmission protocol) example, where we were able to reproduce both, timed and probabilistic verification results from the literature, on the basis of a single MODEST model.

Perspective This work is closely related to the work by AAU reported in D2.1 on Uppaal-Pro. The target is the same. Still we think there is enough difference to justify different places in the deliverable set. Hartmans and Hermanss are considering a language that in principle could be given a semantics in terms of PTA, but they implement an abstract semantics which maps on PA instead. Then they reuse existing algorithms for PA. So, this is work on the semantical/modelling level. They put some emphasis on language features which can be supported, which is not so much the focus of the AAU work. AAU is implementing an algorithm working on PTA directly. An interesting (and obvious) direction for future work is to compare the approaches from AAU and SU.

4 Stochastic hybrid modelling

4.1 Towards modelling and safety verification of probabilistic hybrid automata

Participants

- Holger Hermanns, SU
- Lijun Zhang, SU

jointly with

- Stefan Ratschan, Czech Academy of Science, Czech Republic
- Zhikun She, Beihang University, China

Results The interplay of random phenomena and continuous real-time control deserves increased attention for instance in wireless sensing and control applications. Analysis for such systems thus needs to consider probabilistic variations of systems with hybrid dynamics.

In safety verification of classical hybrid systems one is interested in whether a certain set of unsafe system states can be reached from an initial system state or states. In the probabilistic setting, one asks instead whether the probability of reaching such a set is below some given threshold.

In this work, we have considered probabilistic hybrid systems, hybrid systems where probabilities are added to discontinuous jumps, and have developed a general framework for handling probabilistic safety verification problems. The framework combines and integrates abstraction of classical hybrid systems, and of probabilistic systems for verifying safety of the original probabilistic hybrid system.

Perspective This works lays the ground for ongoing efforts to design a language and tool support for probabilistic and later stochastic hybrid systems.

5 Resources Modelling

5.1 Cost-bounded reachability in priced probabilistic timed automata

Participants

- Jasper Berendsen, ESI/RU
- David Jansen, ESI/RU

jointly with:

- Taolüe Chen, CWI Amsterdam, Netherlands

Results Recently the model of Priced Probabilistic Timed Automata (PPTA) has been put forward, which are timed automata extended with price rates in locations and discrete probabilistic branching. The model is a natural combination of Priced Timed Automata and Probabilistic Timed Automata. In this paper we focus on cost-bounded probabilistic reachability for PPTA, which determines if the maximal probability to reach a set of goal locations within a given price bound (and time bound) exceeds a threshold $p \in [0, 1]$. We prove undecidability of the problem for simple PPTA with 3 clocks. Simple PPTA, a. o., have strictly positive price rates. Undecidability also holds for PPTA with 2 clocks that allow negative price rates. We provide an algorithm using a value iteration scheme, and prove the decidability assuming non-zenoness of cost in PPTA. Our undecidability results show that it is difficult to weaken this assumption.

Perspective The model of PPTAs is highly expressive and potentially very useful to model resource requirements of embedded systems. However, due to the high expressivity many properties are undecidable for PPTAs in general. We believe it is important to complement our ongoing efforts (in WP2 and WP5) on algorithms/tools and case studies for PPTAs by theoretical work in which we explore in which cases analysis of PPTAs is feasible and in which cases it isn't. This will help us to identify subclasses of PPTAs that are both sufficiently expressive to model relevant properties of embedded systems, and are amenable to analysis by tools.

5.2 Infinite runs in weighted timed automata with energy constraints

Participants

- Patricia Bouyer, CNRS
- Ulrich Fahrenberg, AAU
- Kim G Larsen, AAU
- Nicolas Markey, CNRS
- Jiri Srba, CNRS

Results We study the problems of existence and construction of infinite schedules for finite weighted automata and one-clock weighted timed automata, subject to boundary constraints on the accumulated weight. More specifically, we consider automata equipped with positive and negative weights on transitions and locations, corresponding to the production and consumption of some resource (e.g. energy). We ask the question whether there exists an infinite path for which the accumulated weight for any finite prefix satisfies certain constraints (e.g. remains between 0 and some given upper-bound). We also consider a game version of the above, where certain transitions may be uncontrollable. This work is published in [5].

Perspectives Priced timed automata (and games) *with* positive and negative weights is precisely the model underlying the HYDAC case study. The model is clearly within that of (linear) hybrid automata (games) but – as is demonstrated in the paper [5] – with the possibility of obtaining decidability results. From [5] there remains a number of (very natural) open problems that will be attempted tackled within the next year.

5.3 Model-checking one-clock priced timed automata

Participants

- Patricia Bouyer, CNRS
- Kim G Larsen, AAU
- Nicolas Markey, CNRS

Results We consider the model of priced (a.k.a. weighted) timed automata, an extension of timed automata with cost information on both locations and transitions, and we study various model-checking problems for that model based on extensions of classical temporal logics with cost constraints on modalities. We prove that, under the assumption that the model has only one clock, model-checking this class of models against the logic WCTL, CTL with cost-constrained modalities, is PSPACE-complete (while it has been shown undecidable as soon as the model has three clocks). We also prove that model-checking WMTL, LTL with cost-constrained modalities, is decidable only if there is a single clock in the model and a single stopwatch cost variable (i.e., whose slopes lie in 0,1). This work is published in [6].

Perspective In future research we will be considering model checking (one-clock) priced timed automata against weighted alternating temporal logics (WATL), where modalities may quantify over teams of players. We conjecture that this model checking problem will be decidable and will subsume the results on WCTL in [6].

5.4 Optimal infinite scheduling for multi-priced timed automata

Participants

- Patricia Bouyer, CNRS
- Ed Brinksma, ESI
- Kim G Larsen, AAU

Results This work is concerned with the derivation of infinite schedules for timed automata that are in some sense optimal. To cover a wide class of optimality criteria we start out by introducing an extension of the (priced) timed automata model that includes both costs and rewards as separate modelling features. A precise definition is then given of what constitutes optimal infinite behaviours for this class of models, namely an infinite run with minimal (or maximal) limit-ratio between the accumulation of cast and accumulation of reward. We subsequently show that the derivation of optimal non-terminating schedules for such double-priced timed automata is computable. This is done by a reduction of the problem to the determination of optimal mean-cycles in finite graphs with weighted edges. This reduction is obtained by introducing the so-called corner-point abstraction, a powerful abstraction technique of which we show that it preserves optimal schedules. This work is published in [7].

Perspective Optimal infinite runs is highly relevant for several production processes. In fact – in a certain precise sense – this this is exactly what is required in the HYDAC case study. However, compared with the above work, the modeling formalism underlying the HYDAC case study is more expressive including negative as well as positive costs and an opponent to the control strategy to be synthesized. Though the above work shows decidability, there still remains to be designed (and implemented) an efficient zone-based algorithm. As of now the use of optimal infinite runs based on finite (cost- or time-) horizons is used in practice.

5.5 Optimal reachability for multi-priced timed automata

Participants

- Kim G Larsen, AAU
- Jacob I Rasmussen, AAU

Results We prove the decidability of the minimal and maximal reachability problems for multi-priced timed automata, an extension of timed automata with multiple cost variables evolving according to given rates for each location. More precisely, we consider the problems of synthesizing the minimal and maximal costs of reaching a given target location. These problems generalize conditional optimal reachability, i.e., the problem of minimizing one primary cost under individual upper bound constraints on the remaining, secondary, costs, and the problem of maximizing the primary cost under individual lower bound constraints on the secondary costs. Furthermore, under the liveness constraint that all traces eventually reach the goal location, we can synthesize all costs combinations that can reach the goal.

The decidability of the minimal reachability problem is proven by constructing a zone-based algorithm that always terminates while synthesizing the optimal cost tuples. For the corresponding maximization problem, we construct two zone-based algorithms, one with and one without the above liveness constraint. All algorithms are presented in the setting of two cost variables and then lifted to an arbitrary number of cost variables. This work is published in [12].

Perspective Though an efficient datastructure is provided in the above work it still remains to be implemented.

5.6 Discount-optimal infinite runs in priced timed automata

Participants

- Ulrich Fahrenberg, AAU
- Kim G Larsen, AAU

Results Discount-optimal infinites scheduling for priced timed automata has been shown decidable using region-based techniques (so-called corner-point abstraction). Using discounting in optimization criteria is a often used in Control Theory, and leads to a simple fixed-point characterization in the setting of weighted timed automata. The fixed-point characterization suggests an efficient algorithm in contrast to limit-ratio optimality. This work is published in [9].

Perspective Though the fixed-point characterization of the above research suggest an efficient algorithm there is a need to design a zone-based (fixed-point) algorithm. The relationship between discount optimal infinite runs and limit-ratio optimal infinite runs needs further investigation. We conjecture that for discounting factors sufficiently close to 1 the two notions will coincide.

Bibliography

[1] H. Bohnenkamp, P.R. d'Argenio, H. Hermanns, and J.-P. Katoen. Modest: A compositional modeling formalism for real-time and stochastic systems. *IEEE Trans. Soft. Eng.*, 32(10):812–830, October 2006.

[2] H. Boudali, P. Crouzen, B.R.H.M. Haverkort, M. Kuntz, and M.I.A. Stoelinga Architectural dependability evaluation with Arcade *38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'08)*, pp 512-521, IEEE Computer Society 2008.

[3] H. Boudali, P. Crouzen, B.R.H.M. Haverkort, M. Kuntz, and M.I.A. Stoelinga. Arcade - A Formal, Extensible, Model-based Dependability Evaluation Framework. In *13th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'08)*, pp. 243–248, Belfast, Northern Ireland, March 31st - April 4th 2008.

[4] H. Boudali, P. Crouzen, B.R.H.M. Haverkort, M. Kuntz, and M.I.A. Stoelinga. Rich Interfaces for Dependability: Compositional Methods for Dynamic Fault Trees and Arcade models. In *2nd International Workshop on Foundations of Interface Theories (FIT'08)* 2008.

[5] P. Bouyer, U. Fahrenberg, K.G. Larsen, N. Markey and J. Srba. Infinite Runs in Weighted Timed Automata with Energy Constraints. In *Proceedings of the 6th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'08)*, Saint-Malo, France, September 2008, LNCS 5215, pages 33-47.

[6] P. Bouyer, K.G. Larsen, N. Markey. Model Checking One-clock Priced Timed Automata. *Logical Methods in Computer Science* 4(2:9), 2008.

[7] P. Bouyer, E. Brinksma, K.G. Larsen. Optimal infinite scheduling for multi-priced timed automata. *Formal Methods in System Design 32(1)*: 3-23, 2008.

[8] J.-P. Katoen, M. Bozzanol, G. Burte, A. Cimatti, M. le Coroller, V.Y. Nguyen, T. Noll, and X. Olive System and Software Co-Engineering: Performance and Verification In *ESA ADCCS Workshop*, Noordwijk, The Netherlands, 2008.

[9] U. Fahrenberg and K.G. Larsen. Discount-Optimal Infinite Runs in Priced Timed Automata. *INFINITY 2008 10th International Workshop on Verification of Infinite-State Systems,* Toronto, Canada, 23rd of August 2008.

[10] M. Kwiatkowska, G. Norman, D. Parker, and J. Sproston Performance analysis of probabilistic timed automata using digital clocks *Formal Methods in System Design*, 29(1):33–78, 2006.

[11] M. Kwiatkowska, G. Norman, J. Sproston, and F. Wang Symbolic model checking for probabilistic timed automata *Information and Computation*, 205(7):1027–1077, 2007.

[12] K.G. Larsen, J. Illum Rasmussen. Optimal reachability for multi-priced timed automata. *Theor. Comput. Sci.* 390(2-3): 197-213,2008.